Bulletin of Electrical Engineering and Informatics
Vol. 11, No. 5, October 2022, pp. 2645~2656
ISSN: 2302-9285, DOI: 10.11591/eei.v11i5.3886

Chaotic-DNA system for efficient image encryption

Huda Rashid Shakir, Sadiq Abdul Aziz Mehdi, Anwar Abbas Hattab
Department Computer Science, Collage of Education, Mustansiriyah University-Iraq, Baghdad, Iraq

Article Info

Article history:

Received Apr 3, 2022
Revised Jul 7, 2022
Accepted Jul 29, 2022

Keywords:

DNA computing
Hyper-chaotic system
Image encryption
Permutation

ABSTRACT

In order to prevent unwanted access to sensitive data by unauthorized individuals, color images are encoded. Because chaotic-DNA encoding can make information highly secure, it is often employed in image encryption. In this study, a new image encryption technique has been proposed based on a new 4D-chaotic system and DNA computing. The algorithm consists of two phases: in the first phase, the pixel positions are permuted by chaotic sequences. In the second phase, according to the concept of DNA cryptography, a set of operations (like DNA addition, DNA XOR, DNA subtraction, shift right, and shift left) are performed on the DNA encoding sequence. The performance of the suggested algorithm is evaluated through analyses like correlation coefficient, entropy, histogram, and key space. The results show that the encryption method that was exhibited has good encryption performance and high security. For encrypted images, the histogram is fairly uniform, the correlation values between adjacent pixels are very small and close to zero, and the entropy is near to the ideal value of eight. In addition, the proposed system has a very large key space that is equal to 2^{627} keys, which makes it resistant to brute-force, differential, and statistical attacks.

Corresponding Author:

Huda Rashid Shakir
Department of Computer Science, Collage of Education, University of Mustansiriyah-Iraq
Alkadhimiya Street, Baghdad, Iraq
Email: hudarashid@uomustansiriyah.edu.iq

1. INTRODUCTION

With the rapid development of multimedia data (such as audio, video, and images) and its transmission across unprotected channels of communication, information security has become increasingly important to avoid risks and data loss [1]-[3]. Image encryption is the most widely used method of safeguarding the privacy of image data. Because of the unique characteristics of images, like their huge data capacity and strong correlation among pixels [4], [5], several conventional data encryption methods, like advanced encryption standard (AES) data encryption standard and (DES), are not suitable for encrypting digital images [6]-[8]. Therefore, various approaches for encrypting image data have been proposed, the most powerful and widely used of which is chaotic-based cryptography, due to its sensitivity to initial state [6], non-linearity, randomness, ergodicity, and so on [9]-[11], which satisfies the fundamental requirements of cryptography.

In 1998, Fridrich was the first to apply the chaotic system and cryptography theory to the Image Encryption System, which consists of two phases: confusion and diffusion, and this architecture has become the most common and has been adopted by many researchers [12]. The use of deoxyribonucleic acid (DNA) and chaotic system-based combined cryptography to achieve high levels of security, particularly for color images and videos, is a broad field. The DNA molecule has several advantages, including strong parallel processing ability, very-low power consumption, and a high data storage capacity [13]-[15].

Recently, many studies have utilized chaotic systems and DNA coding to encrypt images. Cui *et al*., [16] suggested an image encryption technique built on the hyper-chaotic-Lorenz model and dynamic DNA encoding. This approach uses the secure-hashing-algorithm-SHA-256 technique to produce a shared key in a hyper-chaotic system to create a DNA sequence matrix and a dynamic S-box. Then use SCAN mode and the S-box to confuse the pixel position. The pixel values are scrambled using the DNA sequence array to generate cipher text. Simulation results show that the technique makes keyspace more sensitive and can withstand statistical and differential assaults. Shima and Thanikaiselvan [17] suggested a method of image encryption that makes use of four different algorithms and multiple keys by splitting a single image into four blocks and encrypting them first with DNA as a secret key, then using RSA, then DES, and finally using the Chebyshev algorithm, which results in a high level of security and good image quality.

H. Amani and M. Yaghoobi [18] propose a new 4D-hyper-chaotic dynamic system and a DNA sequence for color image encryption. The two key steps in this strategy are: The logical arrangement of the pixels is changed by employing Arnold's cat map in the first stage; permuted images are then encrypted by employing a combination of DNA sequences with Chen's hyper-chaotic scheme, and an adaptive technique makes this algorithm more complex. The results show that the method that was suggested can protect against brute force and statistical attacks. Huang *et al*., [19] suggested a strategy for encrypting chaotic color images using DNA-coding computations and galois field arithmetic. Firstly, three modified (1D) chaotic maps are presented, each with a bigger key space and improved chaotic features. Second, DNA coding and mathematics are used to increase the cryptosystem's permutation. Finally, the numeration applied to the Galois field provides the effect of pixel diffusion. It shows that the encryption method suggested has a big impact on how well it works, and the numerical results show that it's more secure than some of the most recent cryptosystems.

Because employing only DNA to encode images is insecure, researchers are combining DNA coding with chaotic-systems to improve more secure image encryption techniques. However, image encryption made up of DNA encoding and chaotic systems has certain drawbacks, like the independency of the key generation method from the original image, the limitations of DNA operations, and the slow encryption speed [20]. On the other hand, security concerns in low-dimensional chaos have their drawbacks in the small key size and low security. The key size has to be large enough in order to frustrate brute force attacks [21]. As a result, high-dimensional chaotic systems offer higher security and randomness. In general, chaotic systems include only one positive Lyapunov exponent, but when the chaotic systems have at least two or more positive Lyapunov exponents, they are said to be hyper-chaotic. Hyper-chaotic systems generally have more complex dynamical behaviors than ordinary chaotic systems [22].

To solve the problems mentioned above, a novel 4D- hyperchaotic system and DNA encoding have been suggested. Firstly, the pixel positions are permuted by chaotic sequences. Secondly, according to the concept of DNA cryptography, a number of operations like (DNA addition, DNA XOR, DNA subtraction, shift right, and shift left) are applied to the DNA encoding sequence to encrypt color images and achieve good encryption results.

2. THEORETICAL BACKGROUND

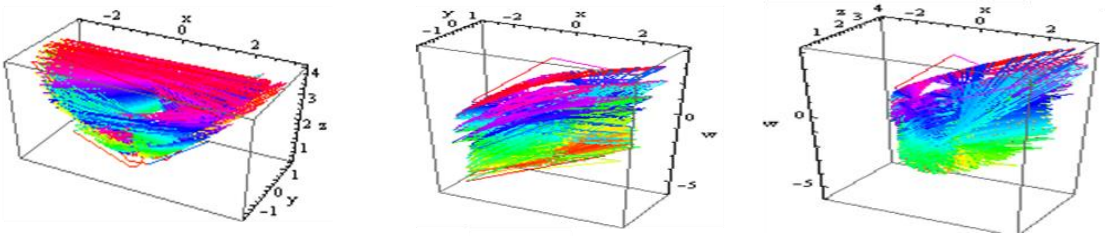
2.1. The novel chaotic system

A new 4D-hyper chaotic system is constructed using a system model represented by the following differential equation:

$$\begin{aligned} \frac{dx}{dt} &= -a\,x - b\,w + c\,y\,z + z\,e^{y} \\ \frac{dy}{dt} &= d\,y + e\,x - f\,x\,z - x\,e^{z} \\ \frac{dz}{dt} &= -g\,z + h\,x\,y \\ \frac{dw}{dt} &= -b\,w + i\,x\,z + j\,y\,z \end{aligned} \tag{1}$$

Where x, y, z, and w called the states of system, t$\in\Re$ and $a, b, c, d, e, f, g, h, i, and\ j$ are positive parameters of the system (1) shows a chaotic attractor in a new four-dimensional chaotic system with parameter values of: *a*=3.1, *b*=2.1, *c*=15.8, *d*=1.1, *e*=16.5, *f*=1.5, g=2.4, h=26.6, i=5.1, and j=12.9, and the initial states of : x(0)=0.2, y(0)=0.4, z(0)=1.5, and w(0)=0.8. The four Lyapunov Exponents of the nonlinear dynamical system (1), with parameters *a*=3.1, *b*=2.1, *c*=15.8, *d*=1.1, *e*=16.5, *f*=1.5, g=2.4, h=26.6, i=5.1, and j=12.9 are obtained as follows: LE_1= 4.05761, LE_2= 0.347562, LE_3=-3.94257 and LE_4=-6.61896. This system contains chaotic features since the highest Lyapunov exponent is positive. Because LE1 and LE2 are

positive Lyapunov exponents, and the two remainders are negative. As a result, the system is hyper-chaotic. Figure 1(a) displays the system's attractors in (x-y-z), Figure 1(b) in (y-x-w), and Figure 1(c) (w-z-z).



(a) (b) (c)

Figure 1. Chaotic attractors, 3-D view (a) (x-y-z), (b) (y-x-w) and (c) (x-z-w)

2.2. DNA computing

Adelman was the first to use DNA computing in cryptography in 1994 to solve the Hamiltonian path problem instead of conventional cryptography. DNA is a molecule that includes the genetic information necessary for any living organism's growth, development, and reproduction. DNA sequences contain of four nucleic acid bases: A (adenine), G (guanine), C (cytosine) and thymine (T). The complementary pairing concept is followed by the nucleotides Adenine and Thymine, Guanine and Cytosine. While A, C, G, and T indicate numerals, they can also represent the decimal digits 0, 1, 2, 3. These four decimal digits are equivalent to the binary numbers 00, 01, 10, and 11, which means that each nucleotide can carry two bits of information. This coding has a total of 4!=24 different encoding methods. However, only eight types of encoding schemes that refer to the complimentary pairing requirement [16], [23], [24] are shown in Table 1. Additionally, Table 2 includes operations for DNA addition, subtraction, and exclusive-or.

Table 1. DNA rules [23]

Rules	1	2	3	4	5	6	7	8
0	A	A	C	C	G	G	T	T
1	G	C	T	A	T	A	G	C
2	C	G	A	T	A	T	C	G
3	T	T	G	G	C	C	A	A

Table 2. The operation of DNA sequences [23]

Addition-DNA

(Add)	A	C	G	T
A	T	A	C	G
C	A	C	G	T
G	C	G	T	A
T	G	T	A	C

Subtraction-DNA

(Sub)	A	C	G	T
A	C	A	T	G
C	G	C	A	T
G	T	G	C	A
T	A	T	G	C

Exclusive-or

(Xor)	A	C	G	T
A	A	C	G	T
C	C	A	T	G
G	G	T	A	C
T	T	G	A	C

3. METHODOLOGY

The proposed method contains two main stages encryption stage (forward stage) and decryption stage (backward stage) as explained in the following paragraphs:

3.1. Encryption stage

The encryption stage passes several steps to produce an encrypted image, starting by splitting the color image into RGB bands (red, green, and blue). At the same time, the initial conditions and parameters are entered into the 4D-chaotic system to generate four chaotic sequences. These sequences are used in the permutation step for each color band. Then DNA encoding is applied to the permutation image produced from the previous step to use in the round function step, which includes operations such as addition, subtraction, and exclusive-or. The fourth chaotic sequence is used for dynamic shifting in the left and right directions. Three rounds are applied to find the final encrypted image as shown in Figure 2.

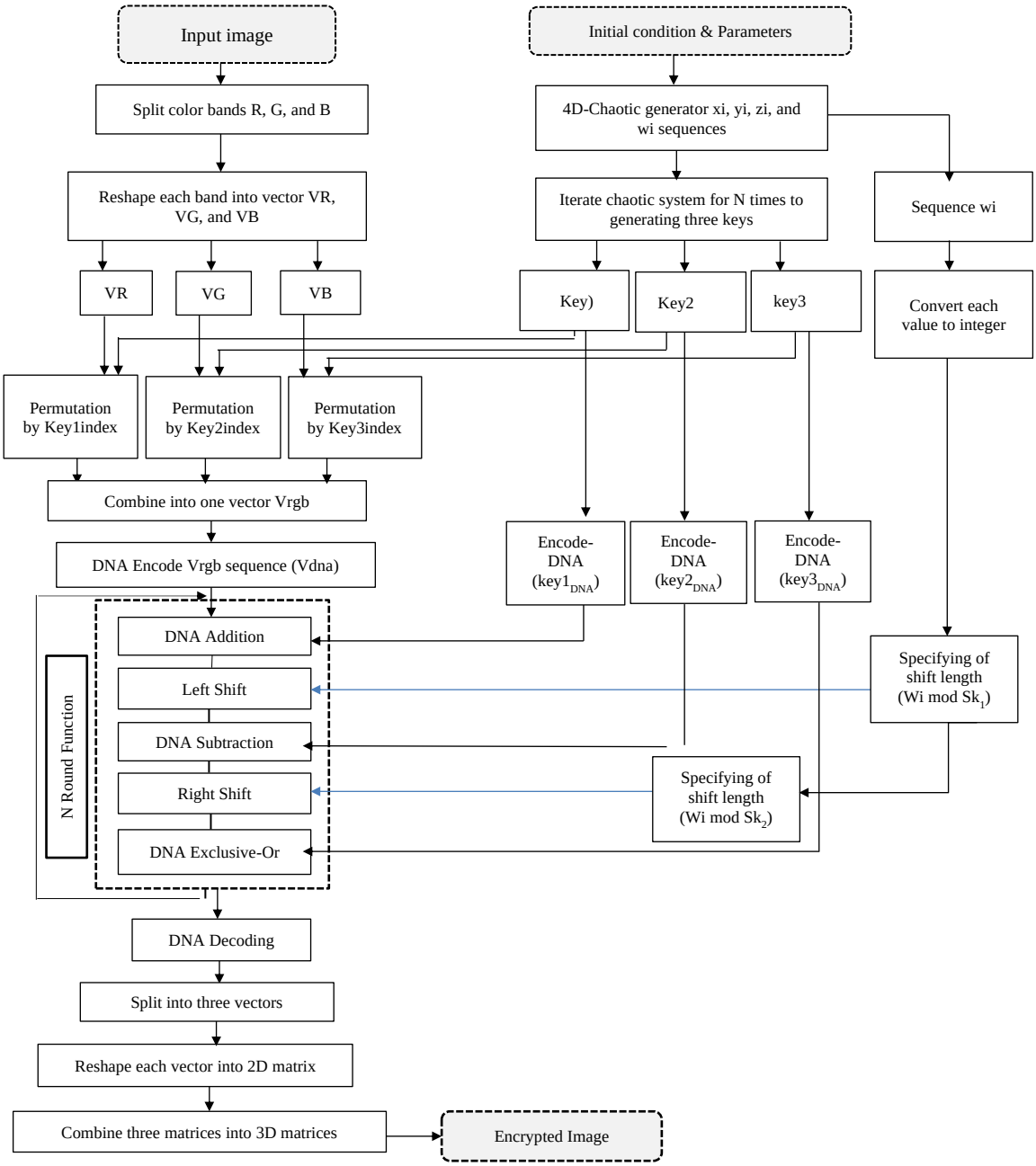


Figure 2. The general framework of encryption stage

3.1.1. Generating 4D chaotic sequence

Depending on the 4D chaotic system, which is generated by entering the parameters and initial conditions, the suggested hyper-chaotic iterates to produce four chaotic- sequences (xi, yi, zi, and wi) of real numbers, which are converted into three vectors as keys (key1, key2, and key3). The size of each vector is equivalent to the size of the original image dimensions (h*w). Table 3 shows a sample of chaotic sequences of real numbers that have been processed to be converted into digits of hexadecimal.

3.1.2. Permutation step

At this stage, the split RGB bands are reshaped into vectors (VR, VG, and VB) and are scrambled based on the chaotic sequences (xi, yi, zi). Each one of the three chaotic vectors will be sorted in ascending order and generate the index for each chaotic sequence ($key1_{index}$, $key2_{index}$, $key3_{index}$) in order to permute the position of each value in the image bands. The first sequence ($key1_{index}$) permutes the red vector (VR1), the

second sequence ($key2_{index}$) permutes the green vector (VG1), and the third sequence ($key3_{index}$) permutes the blue vector (VB1).

Table 3. Samples of 4D chaotic sequences

Generated numbers	Moving floating point	Rounding numbers	Hexadecimal form
0.201437280655153	2014372806.5515	2014372807	7810E3C7
0.202875019921153	2028750199.2115	2028750199	78EC4577
0.204313227427431	2043132274.2743	2043132274	79C7B972
0.205751912809594	2057519128.0959	2057519128	7AA34018
0.207191085709668	2071910857.0967	2071910857	7B7ED9C9
0.208630755776090	2086307557.7609	2086307558	7C5A86E6

3.1.3. DNA encoding

The DNA coding is applied to the result of permutation produced from the previous step by combining three vectors into one vector and converting each value in the vector into binary form, with every two bit converted into one of the DNA symbols A, C, G, and T based on Table 1. The total vector will be a strand of DNA sequence ($Vrgb_{DNA}$) in order to apply it to the DNA operations in the next steps.

3.1.4. Round function of DNA operation

In this step, the strand of DNA sequence ($Vrgb_{DNA}$) is used in DNA operations (addition, subtraction, and exclusive-or). Firstly, a DNA-addition operation is applied between the DNA sequence and the first key ($key1_{DNA}$) (depending on Table 2). Then, we apply the left shift to the addition result depending on the fourth chaotic sequence (wi). Secondly, we performed the subtraction operation between the result from the left shift and the second key ($key2_{DNA}$) (depending on Table 2), and then applied the right shift to the result of subtraction depending on the fourth chaotic sequence (wi). Finally, implement the Exclusive-Or (X-or) operation between the result right shift from the previous step and the third key vector ($key3_{DNA}$). These steps are repeated for N rounds to obtain the final encryption image. Algorithm 1 and Figure 2 display the steps of encryption in detail.

Encryption Algorithm (1)
Input: original image (IM) of size h×w×3, initial conditions(x0, y0, z0, and w0) and parameters(a, b, c, d, e, f, g, h, I, j)
Output: encrypted image (En)
Begin
step1: read (IM) image
step2: split (IM) image into three color bands R, G, and B
step3: assign h←height of IM
assign w←width of IM
Calculate S← h×w
step4: Reshape bands R, G, and B into three vectors VR, VG, and VB
step5: Iterate suggested chaotic system (1) to generate four chaotic sequences (xi, yi, zi, and wi) to get(key1, key2, key3), size of each them ≥ S,
step6: sort sequence xi ascending and find the position (xi) and store its position in index sequence($key1_{index}$)
sort sequence yi ascending and find the position (yi) and store its position in index sequence ($key2_{index}$)
sort sequence zi ascending and find the position (zi) and store its position in index sequence ($key3_{index}$)
step7: permutated VR by ($key1_{index}$) to produce VR1
Permutated VG by ($key2_{index}$) to produce VG1
Permutated VB by ($key3_{index}$) to produce VB1
step8: combine three vectors VR1, VG1, and VB1 into one vector Vrgb
step9: Encode the vector Vrgb into DNA sequence $Vrgb_{DNA}$
step10: Encode the vector key1 into DNA sequence $key1_{DNA}$
Encode the vector key2 into DNA sequence $key2_{DNA}$
Encode the vector key3 into DNA sequence $key3_{DNA}$
step11: Round Function:
-apply addition operation between $Vrgb_{DNA}$ and $key1_{DNA}$ to produce T1
-apply left shift T1 depending on wi sequence (wi mod sk1) to obtain TSleft

-apply subtraction operation between TSleft and Skey2 to produce T2
-apply right shift T2 depending on wi sequence (wi mod sk2) to obtain TSright
-apply Exclusive-Or operation between TSright and Skey3 to produce T3

step12: repeat step11 for N round function
step13: decode DNA sequence T3 to produce T_{final}
step14: split (T_{final}) into three vectors and reshape each vector into matrices (MR, MG, and MB)
step16: concatenate (MR, MG, and MB) to obtained 3D matrix encrypted image (En)
End Algorithm

3.2. Decryption stage

In the decryption stage, all steps are applied to the encrypted image in reverse order. The encrypted image is encoded to a DNA sequence and DNA operations are applied in reverse order, which includes: (X-or, right shift, addition, left shift, and subtraction, respectively), and the number of rounds function is equal to the number of rounds in the encryption stage. The extracted image is then obtained by applying the inverse permutation to the result of the previous step. Algorithm 2 and Figure 3 show the decryption steps in detail.

Decryption Algorithm (2)
Input: Encryption image (En) of size h×w×3, initial conditions(x0, y0, z0, and w0) and parameters (a, b, c, d, e, f, g, h, I, j)
Output: Extracted image (EI)
Begin
step1: read (En) image
step2: split (En) image into three color bands R, G, and B
step3: assign h←height of En
assign w←width of En
Calculate S← h×w
step4: Reshape three color bands into three vectors IV_R, IV_G, and IV_B
step5: Iterate suggested chaotic system (1) to generate three chaotic sequences (xi, yi, zi, and wi) to get(key1, key2, key3), size of each them ≥ S,
step6: combine three vectors IV_R, IV_G, and IV_B into one vector IVrgb
step7: Encode the vector IVrgb in DNA sequence $IVrgb_{DNA}$
step8: Encode the vector key1 in DNA sequence $key1_{DNA}$
Encode the vector key2 in DNA sequence $key2_{DNA}$
Encode the vector key3 in DNA sequence $key3_{DNA}$
step9: Inverse Round function:
-apply Exclusive-Or operation between $IVrgb_{DNA}$ and $key3_{DNA}$ to produce Tx1
-apply Right shift on Tx1 depending on wi sequence (wi mod sk2) to obtain Tx_{right}
-apply subtraction operation between Tx_{right} and $key2_{DNA}$ to produce Tx2
-apply Left shift on Tx2 depending on wi sequence (wi mod sk1) to obtain Tx_{left}
-apply addition operation between Tx_{left} and $key1_{DNA}$ to produce Tx3
step10: repeat step9 for N round function
step11: decode DNA sequence T3 to produce Te_{final}
step12: split (Te_{final}) into three vectors IV_R, IV_G, and IV_B
step13: sort sequence xi ascending and find the position (xi) and store its position in index sequence(key1index)
sort sequence yi ascending and find the position (yi) and store its position in index sequence (key2index)
sort sequence zi ascending and find the position (zi) and store its position in index sequence (key3index)
step14: permutated the vector IV_R by $key1_{index}$ to produce IV_{R1}
Permutated the vector IV_G by $key2_{index}$ to produce IV_{G1}
Permutated the vector IV_B by $key3_{index}$ to produce IV_{B1}
step15: reshape each vector (IV_{R1}, IV_{G1}, IV_{B1}) into matrices (MeR, MeG, and MeB)
step16: concatenate (MeR, MeG, and MeB) to obtained 3D matrix extracted image (EI)
End Algorithm

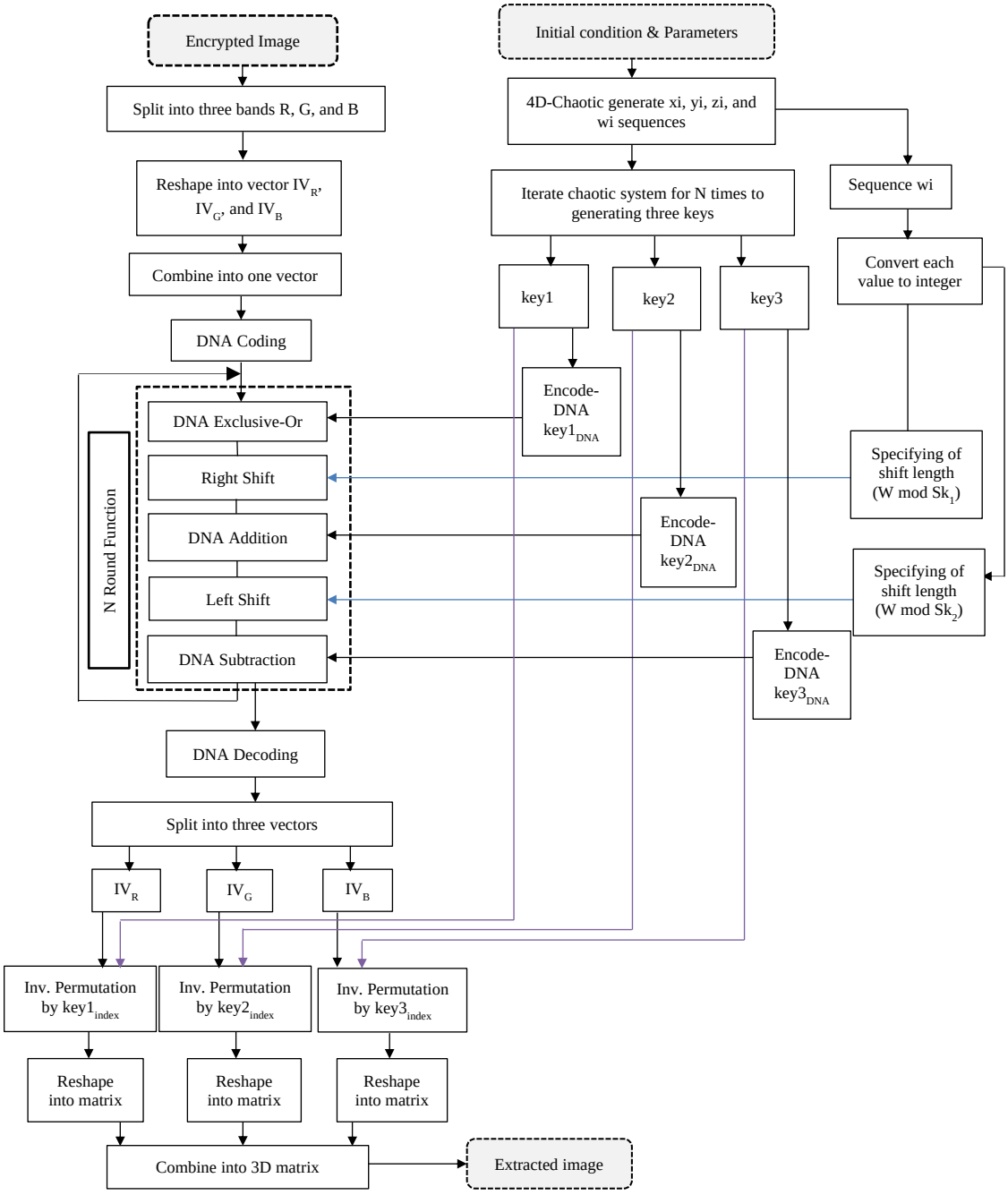


Figure 3. The general framework of decryption stage

4. RESULTS AND DISCUSSION

Several tests are applied to the proposed method to evaluate the efficiency of the encryption suggested algorithm. These tests include key space, histograms, correlation analysis. A set of color images is used for testing and evaluation of results. These tests are illustrated as follows:

4.1. Key space analysis

The key space should be large enough to thwart brute force attacks. An encryption method can use all possible and distinct key values as long as the minimum possible encryption key size is 10128 bits to withstand brute force attacks [23], [25]. In the suggested method, the key space is equal to 2^{627}, which means it is resistant to brute-force attack. Table 4 compares the proposed method's key space results with those of related works.

Table 4. Comparative of key space

Method	Key space value
Proposed method	2^{627}
Ref.[16]	$3.4028 * 10^{74}$
Ref.[18]	2^{514}
Ref.[19]	2^{299}

4.2. Histogram analysis

The histogram shows the visual distribution of pixel values in an image, which is an important aspect to reflect if the algorithm is resistant to statistical analysis. The histogram of the cipher image must be uniform and varied from the corresponding histogram of the original image, which consequently provides no clue for statistical analysis of the encrypted image [26], [27]. Figure 4 shows the histogram tested images before and after encryption.

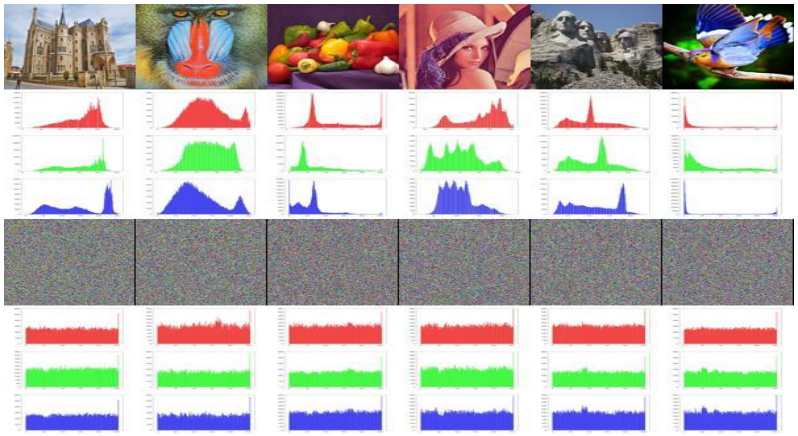


Figure 4. The histogram analysis of proposed method

4.3. Correlation analysis

In general, an image is made up of many pixels. Because adjacent pixels are usually quite similar, they have a high correlation with one another. An ideal image encryption technique would disrupt the intrinsic association between neighboring pixels, making it impossible for an opponent to guess the original image using this information. Normally, the following equation is used to determine the correlation between vertical, horizontal, and diagonal pixels [28]:

$$CC = \frac{N\sum_{j=1}^{N}(x_j \times y_j) - \sum_{j=1}^{N} x_j \times \sum_{j=1}^{N} y_j}{\sqrt{N\sum_{j=1}^{N} x_j^2 - (\sum_{j=1}^{N} x_j)^2)(N\sum_{j=1}^{N} y_j^2 - (\sum_{j=1}^{N} y_j)^2)}} \quad (2)$$

The pixel intensity values of two neighboring pixels are x and y, and the number of pixels is denoted by N. Table 5 shows the correlation test for the plain and encrypted image. Figure 5 shows the correlation test of the suggested method in the (horizontal, vertical, and diagonal) directions. Also, Table 6 displays the comparison results of the correlation test of Lena image with other methods.

Table 5. Correlation test for plain and encrypted image

Horizontal Correlation		Vertical correlation		Diagonal correlation	
Plain image	Encrypted image	Plain image	Encrypted image	Plain image	Encrypted image
0.89285	0.00642	0.89285	0.00642	0.84829	0.00110
0.92566	0.00320	0.92566	0.00320	0.86998	-0.00024
0.98816	0.00423	0.98816	0.00423	0.97477	-0.00504
0.96438	0.00305	0.96438	0.00305	0.94832	-0.00191
0.92188	-0.00211	0.92188	-0.00211	0.85933	-0.00360
0.96362	-0.00126	0.96362	-0.00126	0.92952	-0.00023

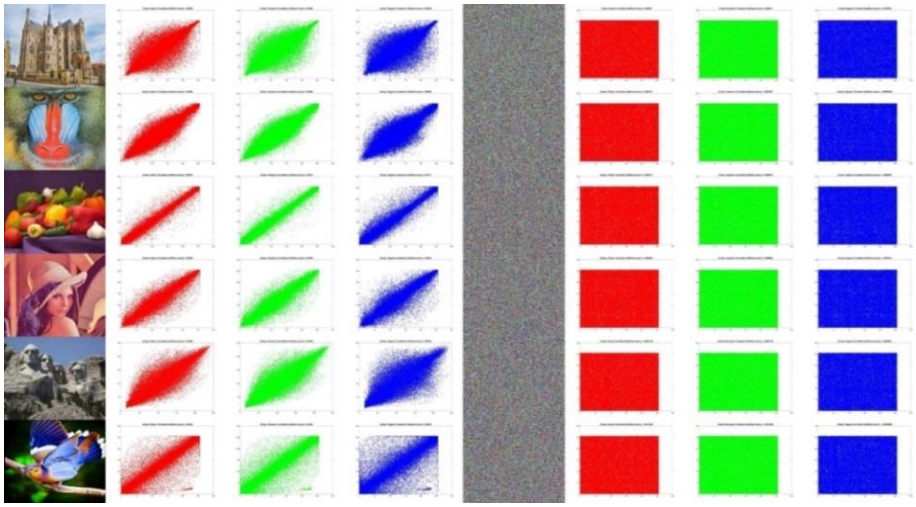


Figure 5. The correlation test of proposed method (horizontal, vertical and diagonal)

Table 6. Comparison results of correlation test lena image with other methods

Lena Encrypted image	Horizontal	Vertical	Diagonal
Proposed method	0.00305	0.00305	-0.00191
[16]	-0.0046	0.0045	-0.0074
[18]	0.00603	0.00476	0.0041
[19]	- 0.0034	0.0021	- 0.0003

4.4. Information Entropy Analysis

Shannon proposed information entropy in 1948, using the thermodynamic idea of entropy to identify the relation among probability and information redundancy in mathematical terms. For a perfect random image, the information entropy value is 8 [29]-[31]. In (3) is the formula for calculating the information entropy of a random information sequence X:

$$Entropy\ E(X) = -\sum_{i=1}^{2^*n} p(X_i)\log\ p(X_i) \quad (3)$$

Table 7 shows the values of the entropy test of images. The results indicate that the information entropy of the encryption images is near to 8, which means that the system is capable of resisting entropy attacks. Table 8 displays the comparison results of the entropy test of the Lena image with other methods.

Table 7. The entropy test of images

Image	Palace	Baboon	Vegetables	Lena	Monuments	Birds
Plain image	7.68523	7.69805	7.43719	7.75155	7.54016	6.97018
Encryption image	7.99857	7.99656	7.99702	7.99987	7.99727	7.99740

Table 8. Comparison results of entropy test Lena image with other methods

Lena encrypted image	Entropy value
Proposed method	7.99987
Ref.[16]	7.9896
Ref.[18]	7.9983
Ref.[19]	7.9971
Ref.[31]	7.929

4.5. Differential attack analysis

The unified average changing intensity (UACI) and the number of pixels change rate (NPCR) are two differential attack metrics used to determine the susceptibility of the original data to minor modifications. Assume the cipher images are C and C' before and after modifying a single pixel in a plain image [32]-[34]. The following is the formula:

$$NPCR = \frac{\sum_{ij} D(i,j)}{W*H} \times 100\% \quad (4)$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \quad (5)$$

W denotes the image's width, while H denotes the image's height; C1 and C2 represent the encrypted images before and after changing one pixel in the original image. Table 9 shows the results of the NPCR and UCAI tests. In addition, Table 10 displays comparison results of the NPCR as well as UACI tests of Lena image with other methods.

Table 9. The NPCR and UCAI test

Image	NPCR	UCAI
Palace	99.61090088	31.24479406
Baboon	99.61242676	29.28272123
vegetables	99.61547852	33.6586567
Lena	99.60699544	33.36560258
monuments	99.62005615	31.6231119
birds	99.60327148	35.36180085

Table 10. Comparison results of The NPCR and UACI test of Lena image with other methods

Lena encrypted image	NPCR	UCAI
Proposed method	99.60699544	33.36560258
Ref.[16]	99.60	28.71
Ref.[17]	98.6	33.1
Ref.[18]	99.53	34.26
Ref.[19]	99.6108	33.4642
Ref.[31]	99.65	32.4966

4.6. MSE and PSNR ratio analysis

As a common criterion for image encryption techniques, the cipher-image should be significantly different from the original image. The difference between plain and cipher images can be assessed using two criteria: the mean square error (MSE) and the peak signal-to-noise ratio (PSNR). Table 11 shows the MSE and PSNR tests and they can be calculated using (6) and (7) [24].

$$PSNR = 20\log_{10}\left(\frac{255}{\sqrt{MSE}}\right)dB \quad (6)$$

$$\mathrm{MSE} = \frac{1}{\mathrm{M}\times\mathrm{N}}\sum_{\mathrm{i,j}} (\mathrm{p}_0(\mathrm{i.j}) - \mathrm{p}_1(\mathrm{i.j}))^2 \quad (7)$$

Table 11. The MSE and PSNR test

Image	Palace	Baboon	vegetables	Lena	Monuments	Birds
MSE	9505.137	8236.518	11357.88	8914.025	8410.986	15437.31
PSNR	3.607009	4.242124	2.89338	3.891629	4.073957	1.440728

5. CONCLUSION

A novel image encryption approach is introduced using a 4D-hyper chaotic system and DNA encoding to achieve a high level of image encryption security. Firstly, chaotic sequences generated by a new 4D-hyperchaotic system are used to permute the pixel positions. Secondly, the pixel values are changed according to DNA operations (like DNA addition, DNA XOR, DNA subtraction, shift right, and shift left) to achieve high diffusion. The algorithm's performance was evaluated using analysis measures such as histogram analysis, key space analysis, correlation coefficient analysis, information entropy analysis, number of pixels change rate (NPCR), unified average changing intensity (UACI), PSNR, and MSE. The results of the tests show that the algorithm is very secure, efficient, and resistant to a lot of different types of attacks. For encrypted images, the histogram is fairly uniform, the correlation values between adjacent pixels are very small and close to zero, and the entropy is close to the ideal value of eight. Also, the NPCR and UACI values are close to the ideal values of (99%) and (33%), respectively. Additionally, the suggested system is extremely sensitive to key changes and has a very wide key space equivalent to 2627 keys, which makes it withstand brute-force, differential, as well as statistical attacks.

REFERENCES

[1] M. Liu and G. Ye, "A new DNA coding and hyperchaotic system based asymmetric image encryption algorithm," *Mathematical Biosciences and Engineering*, vol. 18, no. 4, pp. 3887–3906, 2021, doi: 10.3934/mbe.2021194.

[2] H. Wen, S. Yu, and J. Lü, "Breaking an image encryption algorithm based on DNA encoding and spatiotemporal chaos," *Entropy*, vol. 21, no. 3, pp. 1–18, 2019, doi: 10.3390/e21030246.

[3] S. K. Mutto, D. Anggarwal, and B. Ahuja, "A Secure Image Encryption Algorithm Based on Hill Cipher System," *Bulletin of Electrical Engineering and Informatics*, vol. 1, no. 1, pp. 51–60, 2012, doi: 10.12928/eei.v1i1.226.

[4] K. Xuejing and G. Zihui, "A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system," *Signal Processing: Image Communication*, vol. 80, June 2019, p. 115670, 2020, doi: 10.1016/j.image.2019.115670.

[5] C. Han, "An image encryption algorithm based on modified logistic chaotic map," *Optik*, vol. 181, pp. 779–785, 2019, doi: 10.1016/j.ijleo.2018.12.178.

[6] M. Babu, G. S. Devi, M. Y. Krishna, M. V. Prasanna, and N. Iswarya, "Image Encryption Using Chaotic Maps and DNA Encoding," *Journal of Xidian University*, vol. 14, no. 4, 2020, doi: 10.37896/jxu14.4/206.

[7] S. Fadhel, M. Shafry, and O. Farook, "Chaos image encryption methods: A survey study," *Bulletin of Electrical Engineering and Informatics*, vol. 6, no. 1, pp. 99–104, 2017, doi: 10.11591/eei.v6i1.599.

[8] S. Suri and R. Vijay, "A synchronous intertwining logistic map-DNA approach for color image encryption," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 6, pp. 2277–2290, 2019, doi: 10.1007/s12652-018-0825-0.

[9] S. A. Mehdi, "Image Encryption Algorithm Based on a Novel 4D Chaotic System," *International Journal of Information Security and Privacy*, vol. 15, no. 4, pp. 118–131, 2021, doi: 10.4018/IJISP.2021100107.

[10] A. Susanto *et al*., "Triple layer image security using bit-shift, chaos, and stream encryption," *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 3, pp. 980–987, 2020, doi: 10.11591/eei.v9i3.2001.

[11] Y. Wan, S. Gu, and B. Du "A New Image Encryption Algorithm Based on Composite Chaos and Hyperchaos Combined with DNA Coding," *Entropy (Basel)*, vol. 22, no. 2, p. 171, 2020, doi: 10.3390/e22020171.

[12] Q. Liu and L. Liu, "Color Image Encryption Algorithm Based on DNA Coding and Double Chaos System," *in IEEE Access*, vol. 8, pp. 83596-83610, 2020, doi: 10.1109/ACCESS.2020.2991420.

[13] Z. Azimi and S. Ahadpour, "Color image encryption based on DNA encoding and pair coupled chaotic maps," *Multimedia Tools and Applications*, vol. 79, no. 3–4, pp. 1727–1744, 2020, doi: 10.1007/s11042-019-08375-6.

[14] J. Chen, L. Chen, and Y. Zhou, "Cryptanalysis of a DNA-based image encryption scheme," *Information Sciences*, vol. 520, pp. 130–141, 2020, doi: 10.1016/j.ins.2020.02.024.

[15] B. T. Hammad, A. M. Sagheer, I. T. Ahmed, and N. Jamil, "A comparative review on symmetric and asymmetric DNA-based cryptography," *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 6, pp. 2484–2491, 2020, doi: 10.11591/eei.v9i6.2470.

[16] G. Cui, L. Wang, X. Zhang, and Z. Zhou, "An Image Encryption Algorithm Based on Dynamic DNA Coding and Hyper-chaotic Lorenz System," *International Conference on Bio-Inspired Computing: Theories and Applications*, vol. 952, pp. 226-238, 2018, doi: 10.1007/978-981-13-2829-9_21.

[17] S. Maniyath and V. Thanikaiselvan, "A novel efficient multiple encryption algorithm for real time images," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 2, pp. 1327-1336, 2020, doi: 10.11591/ijece.v10i2.pp1327-1336.

[18] H. R. Amani and M. Yaghoobi, "A New Approach in Adaptive Encryption Algorithm for Color Images Based on DNA Sequence Operation and Hyper-Chaotic System," *Multimedia Tools and Applications*, vol. 78, no. 3, pp. 21537-21556, 2019, doi: 10.1007/s11042-018-6989-y.

[19] L. Huang, S. Wang, J. Xiang, and Y. Sun, "Chaotic Color Image Encryption Scheme Using Deoxyribonucleic Acid (DNA) Coding Calculations and Arithmetic over the Galois Field," *Mathematical Problems in Engineering*, vol. 2020, 2020, doi: 10.1155/2020/3965281.

[20] E. Z. Zefreh, "An image encryption scheme based on a hybrid model of DNA computing, chaotic systems and hash functions," *Multimedia Tools and Applications*, vol. 79, pp. 24993–25022, 2020, doi: 10.1007/s11042-020-09111-1.

[21] X. J. Tong, Z. Wang, M. Zhang, Y. Liu, H. Xu, and J. Ma, "An image encryption algorithm based on the perturbed high-dimensional chaotic map," *Nonlinear Dynamics*, vol. 80, no. 3, pp. 1493–1508, 2015, doi: 10.1007/s11071-015-1957-9.

[22] F. Yu *et al*., "Chaos-based engineering applications with a 6d memristive multistable hyperchaotic system and a 2D SF-SIMM hyperchaotic map," *Complexity*, vol. 2021, no. 1, pp. 1-21, 2021, doi: 10.1155/2021/6683284.

[23] A. Girdhar and V. Kumar, "A RGB image encryption technique using Lorenz and Rossler chaotic system on DNA sequences," *Multimedia Tools and Applications*, vol. 77, pp. 27017–27039, 2018, doi: 10.1007/s11042-018-5902-z.

[24] M. G. A. Malik, Z. Bashir, N. Iqbal and M. A. Imtiaz, "Color Image Encryption Algorithm Based on Hyper-Chaos and DNA Computing," in IEEE Access, vol. 8, pp. 88093-88107, 2020, doi: 10.1109/ACCESS.2020.2990170.

[25] S. C. Wang, C. H. Wang, and C. Xu, "An image encryption algorithm based on a hidden attractor chaos system and the Knuth–Durstenfeld algorithm," *Optics and Lasers in Engineering*, vol. 128, p. 105995, May 2020, doi: 10.1016/j.optlaseng.2019.105995.

[26] D. Ravichandran, A. Banu S, B. K. Murthy, V. Balasubramanian, S. Fathima, and R. Amirtharajan, "An efficient medical image encryption using hybrid DNA computing and chaos in transform domain," *Medical & Biological Engineering & Computing*, vol. 59, no. 3, pp. 589–605, 2021, doi: 10.1007/s11517-021-02328-8.

[27] J. Hao, H. Li, H. Yan and J. Mou, "A New Fractional Chaotic System and Its Application in Image Encryption With DNA Mutation," in *IEEE Access*, vol. 9, pp. 52364-52377, 2021, doi: 10.1109/ACCESS.2021.3069977.

[28] S. A. Mehdi and A. A. Kadhim, "Image Encryption Algorithm Based on a New Five Dimensional Hyperchaotic System and Sudoku Matrix," *2019 International Engineering Conference (IEC)*, 2019, pp. 188-193, doi: 10.1109/IEC47844.2019.8950560.

[29] B. Bouteghrine, C. Tanougast, and S. Sadoudi, "Novel image encryption algorithm based on new 3-d chaos map," *Multimedia Tools and Applications volume*, vol. 80, no. 17, pp. 25583–25605, 2021, doi: 10.1007/s11042-021-10773-8.

[30] Z. Feixiang, L. Mingzhe, W. Kun, and Z. Hong, "Color image encryption via Hénon-zigzag map and chaotic restricted Boltzmann machine over Blockchain," *Optics & Laser Technology*, vol. 135, p. 106610, March 2021, doi: 10.1016/j.optlastec.2020.106610.

[31] H. A. Abdullah and H. N. Abdullah, "FPGA implementation of color image encryption using a new chaotic map," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 13, no. 1, pp. 129–137, 2019, doi: 10.11591/ijeecs.v13.i1.pp129-137.

[32] K. Ma, L. Teng, X. Wang, and J. Meng, "Color image encryption scheme based on the combination of the fisher-yates scrambling algorithm and chaos theory," *Multimedia Tools and Applications*, vol. 80, no. 16, pp. 24737–24757, 2021, doi: 10.1007/s11042-021-10847-7.

[33] M. Roy, S. Chakraborty, K. Mali, D. Roy, and S. Chatterjee, "A robust image encryption framework based on DNA computing

and chaotic environment," *Microsystem Technologies*, vol. 27, 2021, pp. 3617-3627, doi: 10.1007/s00542-020-05120-0.
[34] S. BK and R. GK, "An efficient data masking for securing medical data using DNA encoding and chaotic system.," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 6, 2020, doi: 10.11591/ijece.v10i6.pp6008-6018.

BIOGRAPHIES OF AUTHORS

Huda Rashid Shakir received a B.Sc. in Computer Sciences from Mustansiriyah University, Baghdad, Iraq. Currently, she is studying M. Sc. in Computer Science, College of Education, Department of Computer Science, Mustansiriya University, as well as working in the Iraqi Ministry of Education. She can be contacted at email: hudarashid@uomustansiriyah.edu.iq.

Sadiq Abdul Azizi Mehdi received the B.Sc. in Mathematical Sciences from Mustansiriyah University, Baghdad, Iraq in 1996, M.Sc.in Applied Mathematics Sciences - Modeling and Simulation from Al al-Bayt University, Jordan in 2002, and Ph.D. in Applied Mathematics/Data Cryptography from University of Mustansiriyah, Baghdad, Iraq in 2011. Current position & Functions: computer science from Mustansiriyah University. His research interest is in the fields of Dynamical system, Chaotic system, Chaotic Encryption and Modeling & Simulation. He can be contacted at email: sadiqmehdi71@uomustansiriyah.edu.iq.

Anwar Abbas Hattab received the B.Sc in Computer Science from Baghdad University and her MSc degree in Network Management in 2003 from the Iraq Commission for Computer and Informatics, Institute for Post Graduate Studies in Informatics. Currently she is a lecturer in computer science. Anwar has more than 18 years of experience and has supervised Msc and BSc final year project. Her research interests include cryptography, image processing, data security, network security, and databases. She can be contacted at email: anwarabbas76@uomustansiriyah.edu.iq.